example-business.co.uk

C

Fair

Secure where it counts, needs some hardening.

What your grade means

Your site is genuinely secure where it counts (HTTPS, a valid certificate, no exposed files). It is mainly missing some hardening, like the full set of security headers. A normal, respectable result for a small-business site, and very fixable. Every issue you fix moves your grade up.

3	1	6	29
to fix when you can	quick tidy-ups	optional extras	checks passed

Good news first

✓ A secure, encrypted connection
✓ No private files left exposed
✓ A good sending reputation

Fix these first

Details and fixes on the next page

1	**HSTS (Strict-Transport-Security)** Who fixes it: your web person	When you can
2	**Content-Security-Policy** Who fixes it: your web person	When you can
3	**DMARC email anti-spoofing policy** Who fixes it: your web or IT person	When you can

How the grade works

A — Excellent
Strong foundations across the board.

B — Strong
Fundamentally secure, a few minor gaps.

C — Fair (yours)
Secure where it counts, needs some hardening.

D — Needs work
Several real issues worth fixing soon.

E — At risk
A serious problem to fix as a priority.

WHAT TO FIX

The 3 issues worth fixing

Each one in plain English: what it is, why it matters, the fix, and who usually makes it.

HSTS (Strict-Transport-Security)

Your web person · When you can

Your site doesn't yet tell browsers to always use the secure version, so a visitor's very first connection can be pushed onto an insecure one.

Why it matters: On shared Wi-Fi or a compromised router, an attacker can quietly downgrade a visitor to the insecure http:// version and read or alter logins and form data.

Fix: Send a Strict-Transport-Security header with a real max-age, e.g. "max-age=31536000; includeSubDomains".

Content-Security-Policy

Your web person · When you can

Your site is missing a rule that limits which code is allowed to run, a rule that helps block injected or malicious scripts.

Why it matters: A single injected script - from a vulnerable plugin, ad or comment - can run in your visitors' browsers to steal logins, card details or redirect them elsewhere.

Fix: Add a Content-Security-Policy header. Start in report-only mode, then enforce once tuned.

DMARC email anti-spoofing policy

Your web or IT person · When you can

Your domain doesn't tell email providers to block messages that fake your address, so criminals can impersonate you to your customers.

Why it matters: Spoofed email pretending to be you isn't blocked, so phishing in your name still reaches inboxes.

Fix: Publish a DMARC TXT record at _dmarc, starting with "v=DMARC1; p=none" and tightening over time.

EVERYTHING ELSE

Tidy-ups and optional extras

Tidy-up	**DKIM key strength** Fix: Generate a new 2048-bit DKIM key with your email provider, publish it, then retire the old selector.
Optional	**MTA-STS (encrypted email delivery)** Fix: Publish an MTA-STS policy to require TLS for inbound mail.
Optional	**Lookalike domains** Fix: Check who owns each one. If any are not yours and look like they target your customers, report them to your registrar and warn your customers.
Optional	**DNSSEC** Fix: Ask your DNS provider to enable DNSSEC for example-business.co.uk.
Optional	**CAA certificate restriction** Fix: Add a CAA DNS record naming the certificate authority you use (e.g. letsencrypt.org).
Optional	**security.txt disclosure contact** Fix: Add a /.well-known/security.txt with a Contact: line (see securitytxt.org).
Optional	**Third-party script integrity (SRI)** Fix: Add an integrity="sha384-…" attribute to third-party <script> tags where the provider supports it, or self-host the file.

The 29 checks that passed

HTTPS / encryption in transit · Certificate matches the domain · No common sensitive files exposed · No website backups left in the open · Signs the site has been hacked · IP reputation / blocklists · TLS certificate expiry · HTTP redirects to HTTPS · Clickjacking protection (X-Frame-Options) · Cookie security flags · WordPress plugins kept up to date · SPF email anti-spoofing record · Modern TLS only · Directory listing disabled · Cookie consent for tracking · WordPress theme up to date · SPF record within the lookup limit · Mail server accepts encrypted delivery · MIME-sniffing protection (X-Content-Type-Options) · Referrer-Policy · Permissions-Policy · DKIM email signing · Domain registration current · No mixed (insecure) content · Server software version exposure · X-Powered-By disclosure · Domain age · Platform detected · Outside scripts on the home page

WHAT HAPPENS NEXT

Want us to sort it out?

Expect Best can make these changes with whoever runs your website, or keep checking the site for you every week, with a report every month, and tell you straight away if anything new comes up.

Ethan Wetherall
ethan@ebsecurity.co.uk
ebsecurity.co.uk

About this report: it covers what anyone can see from the public side of example-business.co.uk on 6 November 2026. We didn't log in or try to get past anything. It isn't a penetration test and doesn't look inside your server or your files. EB Security is run by Expect Best Ltd, A34 Arena Business Park, Holyrood Close, Poole, Dorset, BH17 7FJ.